

REMARKS

Claims 17-66 and 73-122 are pending in the present application. Claim 113 has been amended as a result of this Response. Claims 17, 22, 27, 32, 37, 42, 47, 52, 57, 62, and 113-122 are independent claims.

CLAIM OBJECTIONS

Claim 113 has been objected to due to a minor informality. Applicants have amended Claim 113 to correct this minor error. Reconsideration and withdrawal of this objection is respectfully requested.

35 U.S.C. § 103(A) LIDL/QUISQUATER/RIVEST REJECTION

Claim 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public -Key Cryptosystem, 1982); and Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest. This rejection insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

In the Office Action mailed November 3, 2004, the Examiner asserts that Lidl discloses splitting a message into blocks, Quisquater discloses the use of two large prime numbers in a parallel processing technique in order to increase speed, and Rivest utilizes two large random prime numbers in order to improve security.

Applicants respectfully assert that independent claim 17 recites a method for establishing cryptographic communications utilizing three or more random and distinct prime numbers. None of Lidl, Quisquater nor Rivest teaches suggest utilizing three or more

random distinct prime numbers. Accordingly, Applicants respectfully submit that independent claim 17 is patentable over this combination for at least this reason.

Further, Applicants respectfully submit that, in formulating the rejection of independent claim 17, in view of Lidl, Quisquater, and Rivest, the Examiner picks and chooses various portions of these three publications to piece together the subject matter of the present claims.

The Examiner has asserted that Quisquater attempts to solve a speed problem and Rivest attempts to solve a security problem. However, the Examiner has failed to establish why one of ordinary skill in the art would combine Lidl, Quisquater, and Rivest, given that Quisquater is directed to increasing speed and Rivest is directed to increasing security.

In the Office Action mailed November 3, 2004, the Examiner appears to assert that increased speed and increased security are generally features that one of ordinary skill in the art would want to implement in any encryption algorithm, and therefore, one of ordinary skill in the art would combine the increased speed teachings of Quisquater with the increased security teachings of Rivest.

However, Applicants respectfully submit that there are hundreds, if not thousands, of publications in the encryption art directed to increasing speed and hundreds, if not thousands, of publications in the encryption art directed to increasing security. The Examiner has failed to establish why one of ordinary skill in the art would specifically pick the increased speed teaching of Quisquater and/or the increased security teaching of Rivest, with the message division technique of Lidl. Accordingly, Applicants respectfully submit that this rejection is fatally deficient for at least this reason.

For the reasons set forth above, the Examiner has not established motivation to combine, as Rivest is concerned with increased security, Quisquater with increased speed,

and Lidl is nothing more than a basic textbook. Applicants respectfully submit that the Examiner's combination of references is deficient this reason.

35 U.S.C. § 103(A) LIDL/QUISQUATER/RIVEST/DING ET AL. REJECTION

Claims 18-66 and 73-92 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public -Key Cryptosystem, 1982); and Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978. This rejection insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

In formulating this rejection in view of Lidl, Quisquater, Rivest, and Ding, the Examiner again picks and chooses various portions of four publications to piece together the subject matter of the present claims. In Applicants previous responses, Applicants argue that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Lidl, Quisquater, Rivest, and Ding in order to piece together the invention recited in the presently claims.

With respect to Ding, et al., Applicants still cannot find any reason on the record why one of ordinary skill in the art would combine Ding with any of Lidl, Quisquater, or Rivest and the Examiner has still failed to present such a reason. Although Ding is generally related to the Chinese Remainder Theorem and application in computing, coding, and cryptography, the Examiner has failed to establish any concrete reasons why one of ordinary skill in the art would combine Ding with any of Lidl, Quisquater, or Rivest. In paragraph 62 of the Office Action of November 4, 2004, the Examiner asserts:

“ . . . The Ding supplies the details of a recursive algorithm which those in the art would have needed in order to implement the Lidl/Quisquater/Rivest combination.”

Applicants respectfully assert that this passage is not motivation. Assuming one of ordinary skill in the art was looking to implement the Lidl/Quisquater/Rivest combination, which Applicants do not admit, there is nothing in the Examiner's rejection that indicates why one of ordinary skill in the art would select Ding to provide such a teaching. Accordingly, Applicants respectfully submit that the Examiner's rejection is fatally deficient for at least this reason.

35 U.S.C. § 103(A) RSA/RIVEST/QUISQUATER/KNUTH REJECTION

Claim 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rivest et al. (US 4,405,829 A) henceforth RSA, and further in view of Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest; Quisquater, Fast Decipherment Algorithm for RSA Public-key Cryptosystem and further in view of Knuth, The Art of Computer Programming, Vol. 2, page 179. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

In formulating the rejection of claim 17 in view of RSA, Rivest, Quisquater, and Knuth, the Examiner again picks and chooses various portions of the four publications to piece together the subject matter of the present claim. In Applicants previous responses, Applicants argue that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of RSA, Quisquater, Rivest and Knuth, in order to piece together the invention recited in the presently pending claim.

In paragraph 64, which is the only motivation advanced by the Examiner with respect to Knuth, the Examiner offers reasons why one of ordinary skill in the art would have been motivated to combine Knuth with RSA/Rivest/Quisquater. The Examiner asserts that Knuth:

“is a well-known reference for computational methods and was used to expand on what the prior art RSA, Rivest, and Quisquater in particular how the algorithms are applied in these references, that is fill in the details.”

Applicants respectfully submit that just because a reference’s teachings are well-known, is insufficient motivation for combining those allegedly well-known teachings with other prior art. Accordingly, Applicants respectfully submit that the Examiner’s argument that the teachings of Knuth are well-known fails to provide motivation for combining Knuth with the RSA/Rivest/Quisquater combination. Applicants further respectfully submit that the Examiner has failed to establish any motivation as to why one of ordinary skill in the art would combine RSA, Rivest, and Quisquater in the first place. In an attempt to establish motivation for combining these three publications, in paragraph 64, the Examiner asserts:

“while they are not identical they are authored by the same authors and thus are used to get a better understanding of their invention.”

Applicants respectfully submit that it is well-settled U.S. patent law, common authorship or inventorship is not per se motivation to combine. Accordingly, Applicants respectfully submit that the Examiner’s rejection is fatally deficient.

35 U.S.C. § 103(A) RSA/QUISQUATER/RIVEST/DING REJECTION

Claims 18-66 and 73-92 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rivest et al. (US 4,405,829 A) henceforth RSA, and further in view of Quisquater, Fast Decipherment Algorithm for RSA Public-Key Cryptosystem, 1982; and Rivest et al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et al. The Chinese Remainder Theorem, World Scientific. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed.

For reasons set forth above, Applicants respectfully submit that the Examiner is merely picking and choosing various features of RSA, Quisquater, Rivest, and Ding, in order to piece together the subject matter of the present claims. For reasons set forth above, Applicants continue to assert that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose the various teachings of RSA, Quisquater, Rivest, and Ding in order to piece together the inventions recited in the presently pending claims. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

35 U.S.C. § 103(A) NEMO/RIVEST/QUISQUATER REJECTION

Claims 17 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996; Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest; and Quisquater, Fast Decipherment Algorithm for RSA Public-key Cryptosystem, 1982. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

The Examiner, in paragraph 59 of the outstanding Office Action, has clarified his reliance on the Nemo paper. In particular, the Examiner has stated that he is not relying upon the Nemo paper as a traditionally printed magazine, but rather, is relying on the Nemo paper as an electronic publication.

MPEP § 2128 states that an electronic publication may be considered to be a printed publication within the meaning of 35 U.S.C. § 102(a) and (b) provided the publication was accessible to persons concerned with the art to which the document relates. The Examiner has not established that the Nemo paper was accessible to anyone, let alone persons concerned with the art to which the document relates.

Applicants respectfully assert that the Nemo paper was made available to one of the inventors of the present application, after the filing date of the present application. As soon as the Nemo paper was made available to one of the inventors of the present application, an Information Disclosure Statement citing the Nemo paper was filed. Applicants point out that the Nemo paper was cited without a date, because the inventor of the present application, to which the Nemo paper was made aware, was unsure of the publication date, or even if publication was made.

Applicants respectfully submit that the inventors of the present application have met their duty of disclosure and it is the duty of the Examiner to establish that the Nemo paper is in fact prior art under 35 U.S.C. § 102(a) or (b).

In order to do so, the Examiner must establish that the Nemo paper was accessible to persons concerned with the art to which the document relates and that access predates the filing date of the present application. To date, the Examiner has not established either.

Applicants have and continue to assert that the Nemo paper was not accessible to persons concerned with the art to which the documents relate prior to the effective filing date of the present invention. As a result, the Nemo paper is neither 35 U.S.C. § 102(a) nor 35 U.S.C. § 102(b) prior art.

The Examiner continues to insist that the so-called “copyleft” protocol is by itself, sufficient evidence to establish: 1) the Nemo paper’s dissemination to the public and 2) the date on which such dissemination occurred.

However, Applicants have conducted a quick and rudimentary search of the USPTO’s Patent Database (www.uspto.gov) from 1976 to the present and have discovered that not one issued U.S. Patent in that time period with a “copyleft” article or publication as a prior art publication. Accordingly, Applicants respectfully assert that the “copy left” protocol is not

recognized as sufficient to establish either publication or availability, by the U.S. Patent and Trademark Office.

The Examiner further cites MPEP § 2121.01, which the Examiner states requires a presumption that a reference's attributes are actually enabled in its entirety, unless evidence to the contrary is presented.

Applicants are unsure whether the Examiner is referring to the teachings in the Nemo paper or the qualifications of the Nemo paper as prior art. Applicants respectfully submit that the fact that the Nemo paper was submitted with a pseudonym, in a fictitious publication, seriously calls into question the Nemo paper's "copyright" date. Since neither the author nor the publication is genuine, Applicants assert that it is most likely that the publication date is also not authentic. The Examiner has failed to establish that it is.

With respect to the teachings of the Nemo paper, the Examiner continues by asserting that the Nemo paper discloses a mathematical and universal truth and even if Applicants were to swear behind the August 19, 1996 date, the Nemo paper would still be admissible as prior art. Applicants respectfully assert that the Examiner's is relying upon the Nemo paper for teaching the use of three prime factors in a cryptosystem. Irrespective of whether the Nemo paper also teaches mathematical and universal truths, the fact that a cryptosystem utilizes three prime factors is not a universal truth, and in fact is part of Applicants invention. Applicants need do nothing more than point to Rivest and Quisquater to support their position that the use of three prime factors is not a universal truth, because both Quisquater and Rivest utilize only two prime factors.

In summary, Applicants respectfully submit that even if the Examiner is relying upon the Nemo paper as an electronic publication, the Examiner has still failed to establish that the Nemo paper was accessible to persons concerned with the art to which the document relates before Applicants effective U.S. filing date. The fact that one of the inventors of the present

application became aware of the Nemo paper after the filing date of Applicants U.S. patent application does not shift the burden to Applicants to establish that the Nemo paper was publicly available before Applicants filing date. That burden is still on the Examiner.

The Examiner has attempted to avoid his burden by relying on a protocol, namely the “copyleft” protocol, which is clearly not accepted by the USPTO as necessary evidence to establish public availability of a prior art reference. Accordingly, Applicants respectfully assert that all rejections rely on the Nemo paper are fatally deficient for at least this reason.

35 U.S.C. § 103(A) NEMO/QUISQUATER/RIVEST/DING REJECTION

Claims 18-66 and 73-122 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996, and further in view of Quisquater, Fast Decipherment Algorithm for RSA Public -Key Cryptosystem, 1982); Rivest et al., A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et al. The Chinese Remainder Theorem, World Scientific. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

Applicants respectfully submit that this rejection be withdrawn for at least the reasons set forth above with respect to the Nemo paper above.

CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance of each of claims 17-66 and 73-122 in connection with the present application is earnestly solicited.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicants hereby petition for a one (1) month extension of time for filing a reply to the outstanding Office Action and submit the required \$120.00 extension fee herewith.

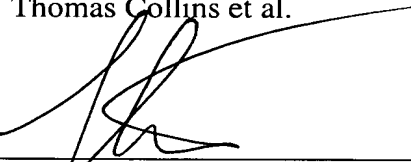
Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact John A. Castellano at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-2025 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

Thomas Collins et al.

By



John A. Castellano, Reg. No. 35,094
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/krf